Insight & Atelier :

Outils et méthodes d'investigation sur la blockchain

SET IN STONE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté
Égalité
Fraternité

CREOGN
CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

01/06/23

ID CARD

2

Set In Stone

› Notre Offre:
Solution de collaboration qui répond à des exigences de sécurité des entreprises, basée sur la blockchain.

› Focus Technologique : Blockchain & enjeux de cyber sécurité

› Localisation : Paris, France

Intervenant

Thomas BENOIT
CEO

> Membre du GT “Securité des CryptoActifs” au Campus Cyber
> Station F alumni
> Computer Engineer diplômé de GeorgiaTech Atlanta & ESIEE Paris

Écosystème

CAMPUS CYBER

Systematic
Paris Region Deep Tech Ecosystem

STATION F

OVH
Startup Program

Chain Accelerator

Be innovative, Be safe, Build with

SET IN STONE LAB

Be innovative, Be safe, Build with SET IN STONE LAB

SET IN STONE LAB renforce la sécurité des applications blockchains, de la première ligne de code à sa maintenance, pour les développeurs qui œuvrent à démocratiser le web3 dans une ère où les cyberattaques se multiplient dans ce secteur.

Be innovative, Be safe, Build with SET IN STONE LAB

Grâce à nos Insights, suivez l’évolution des vulnérabilités du Web3 et appliquez les meilleurs solutions.

INSIGHT 01 – CREOGN - 01/06/23
Outils et méthodes d’investigation sur la blockchain

Sommaire

I. Introduction aux Outils et Méthodes

L’objectif : Nous allons réaliser de l’Open Source Intelligence (OSINT). Le renseignement en sources ouvertes englobe l'exploitation de sources d'information accessibles à tout un chacun (sites web, articles, journaux, conférences…)

Source d’information : Les informations que l’on retrouve dans le registre des transactions d’une blockchain.

💡 De nombreux registres de transactions sont transparents et lisibles par tous les utilisateurs. C’est par exemple le cas du Bitcoin et de l’Ethereum, les deux réseaux blockchains les plus importants à ce jour.

Usages de la lecture des registres de transactions :

- **Investissement :** Anticiper des mouvements financiers et mieux positionner ses investissements
- **Gestion des fonds d’un utilisateur :** Aider un utilisateur à suivre l’activité de l’ensemble de ses wallets
- **Enquête :** Identifier et collecter des traces sur des flux financiers malveillants

I. Introduction aux Outils et Méthodes

Informations lisibles dans une transaction :

🕐 Timestamps : (Date) : Le numéro de bloc du registre blockchain qui définit la date d'exécution de la transaction

🆔 Hash : (Identifiant) : L'identifiant de la transaction

🧑 Adresse de l'émetteur : L'adresse du portefeuille de l'émetteur de la transaction

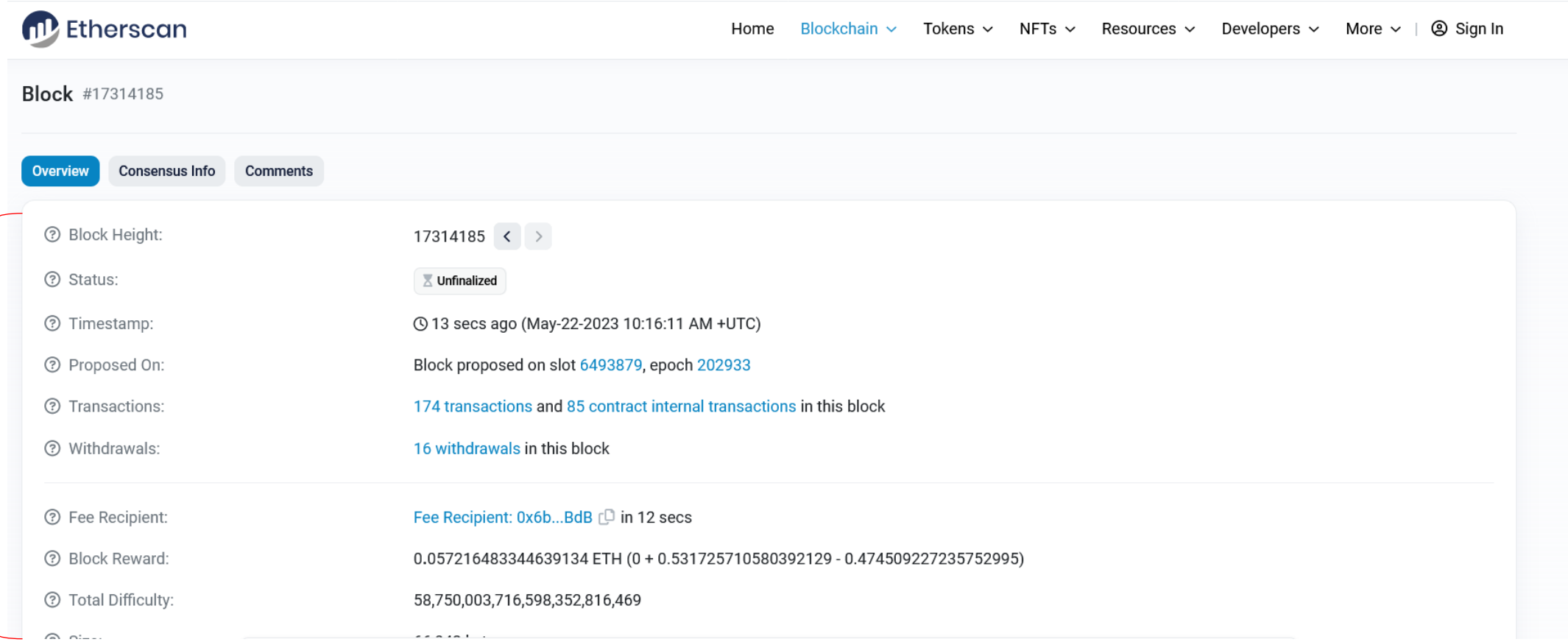
🧑 Adresse du destinataire : L'adresse du portefeuille de l'utilisateur qui reçoit la transaction

💸 Actual Fee (Frais) : Le coût des frais de transaction

💰 Value : (Valeur) : Le montant de la transaction

☑ Transaction Receipt Status : (Statut de la transaction) : Indique si la transaction a été validée par le réseau ou au contraire est en cours de validation, voire a été refusée.

Informations lisibles dans une transaction (un exemple sur EtherScan) :



🎯 Identifier un utilisateur avec un registre blockchain comme source d'information :

Via l'adresse de son portefeuille (communément appelé Wallet).

📏 Son format :

- **Brut : Une adresse sous la forme d'un Hash :**
  Exemple sur Ethereum : « 0xeE0e3B6a2d41cE48B6077f70574874c0F53AdFEA »
- **Nom de domaine :**
  Exemple sur Ethereum : « exemplepoursession.eth »

🚨 Attention :

- Il est commun qu'un utilisateur détienne plusieurs wallets et donc plusieurs adresses
- Sur certain réseau, comme Ethereum, les formats d'adresses sont aussi utilisés pour les smartcontracts (une application décentralisée).

I. Introduction aux Outils et Méthodes

Exemples d'outils pour analyser les registres de transactions blockchains :

Block Explorer

BlockSec MetaDock · Bitquery · Blockstream Explorer · Etherscan · BlockSec Phalcon · Ethplorer · mempool.space · BscScan A product of Etherscan · OKLINK

DeFi

bubblemaps · MESSARI · Dune

Analysis

Chainalysis · BlockSec MetaSleuth · IntelligenceX · breadcrumbs

Wallet

BITCOIN WHOS WHO · WalletLabels · ScamSearch

NFT

NFT Finder · compass · TON NFT EXPLORER

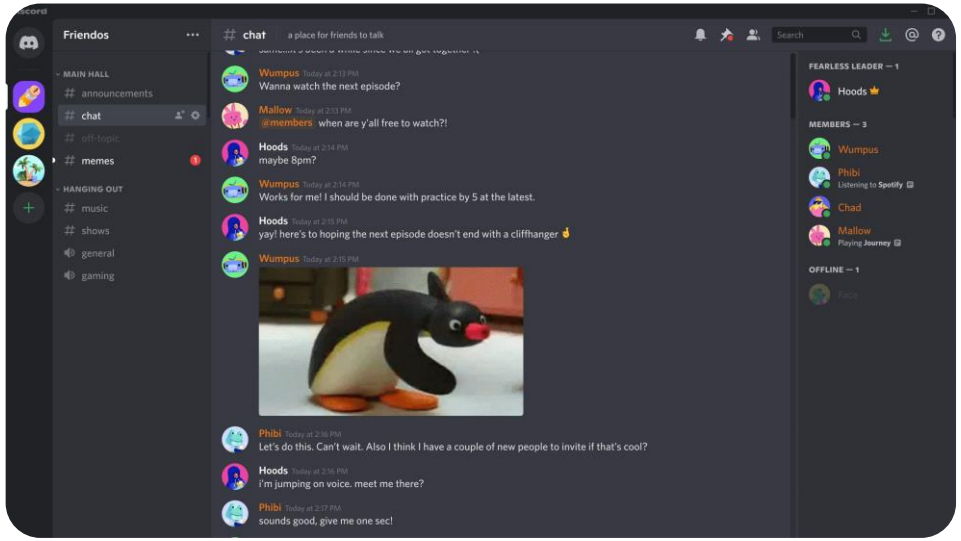
Exploit Alerts

Forta explorer · CERTIK · SLOWMIST · AvengerDAO

Passons à un exemple :
Analysons une attaque de Phishing avec l'outil MetaSleuth.

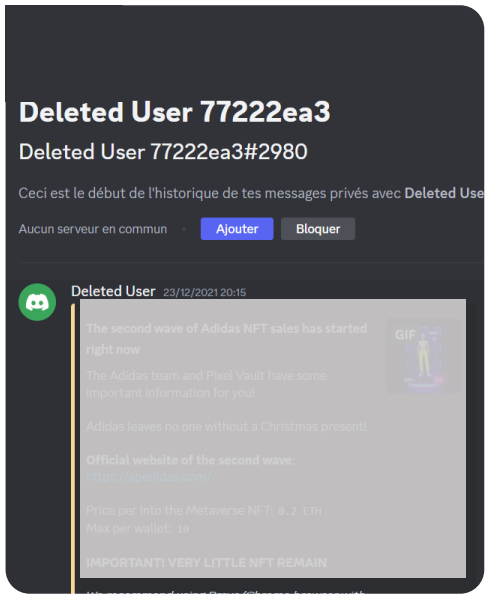
II. Atelier

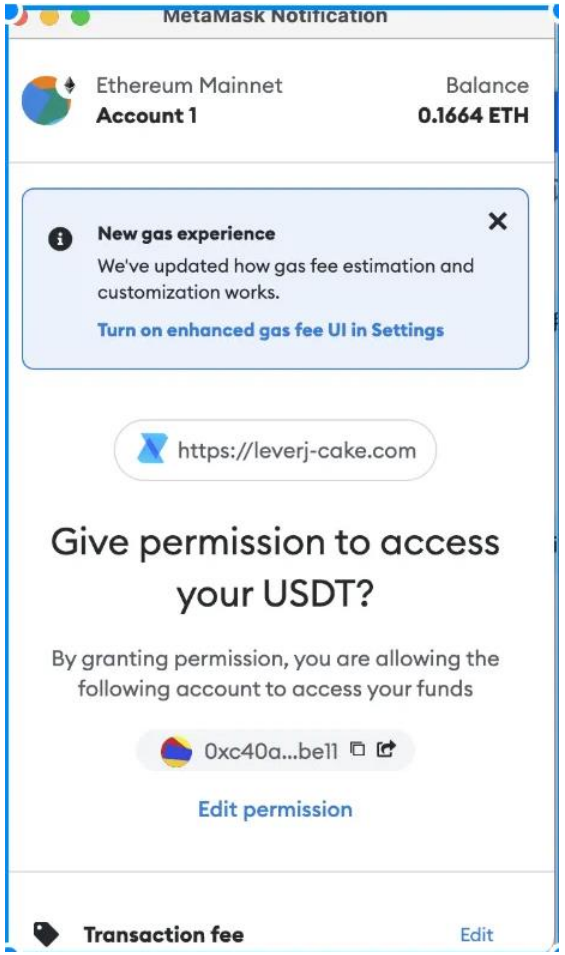
Mathieu, victime d'une attaque de phishing



II. Atelier

Mathieu, victime d'une attaque de phishing





Mathieu, vient d'être victime d'une attaque de phishing !

L'attaquant s'est appuyé sur un biais cognitif appelé FOMO (peur de manquer une opportunité) pour piéger Mathieu.

Les transactions de cette attaque de phishing ont eu lieu sur la blockchain.

Comment pouvons-nous analyser le registre de transactions pour identifier l'auteur de cette attaque ?

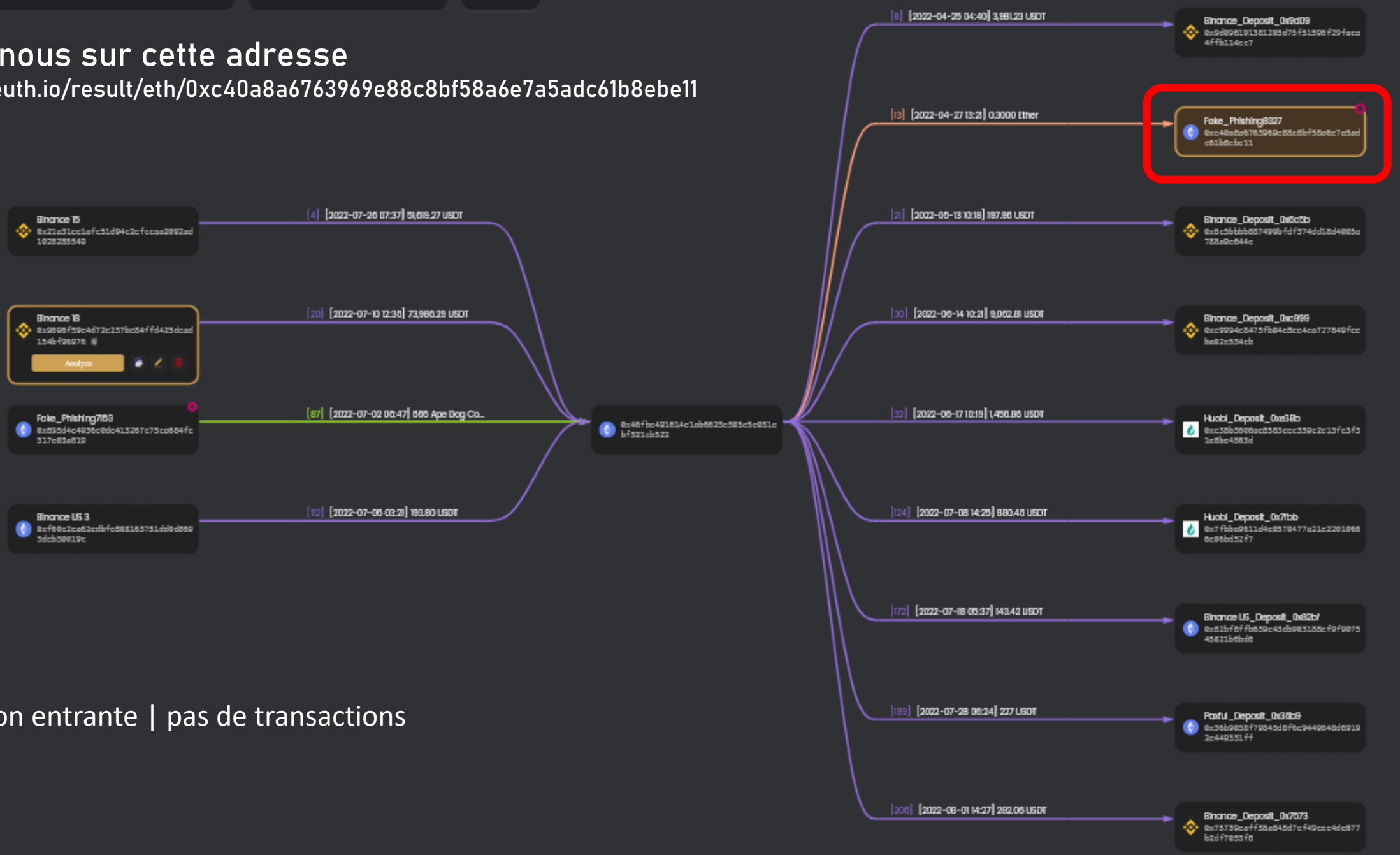
II. Atelier

Notre carnet d'enquête :

- L'adresse où les fonds de Mathieu ont transité : 0xc40a...be11

Penchons nous sur cette adresse

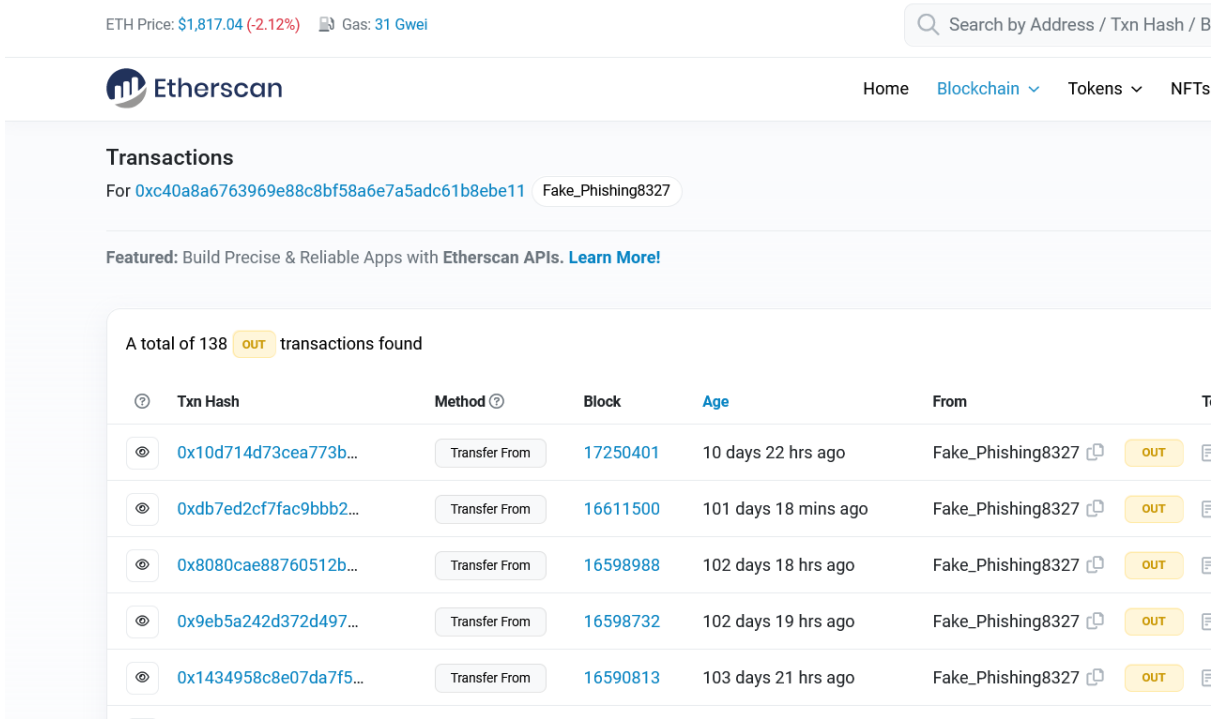
https://metasleuth.io/result/eth/0xc40a8a6763969e88c8bf58a6e7a5adc61b8ebe11

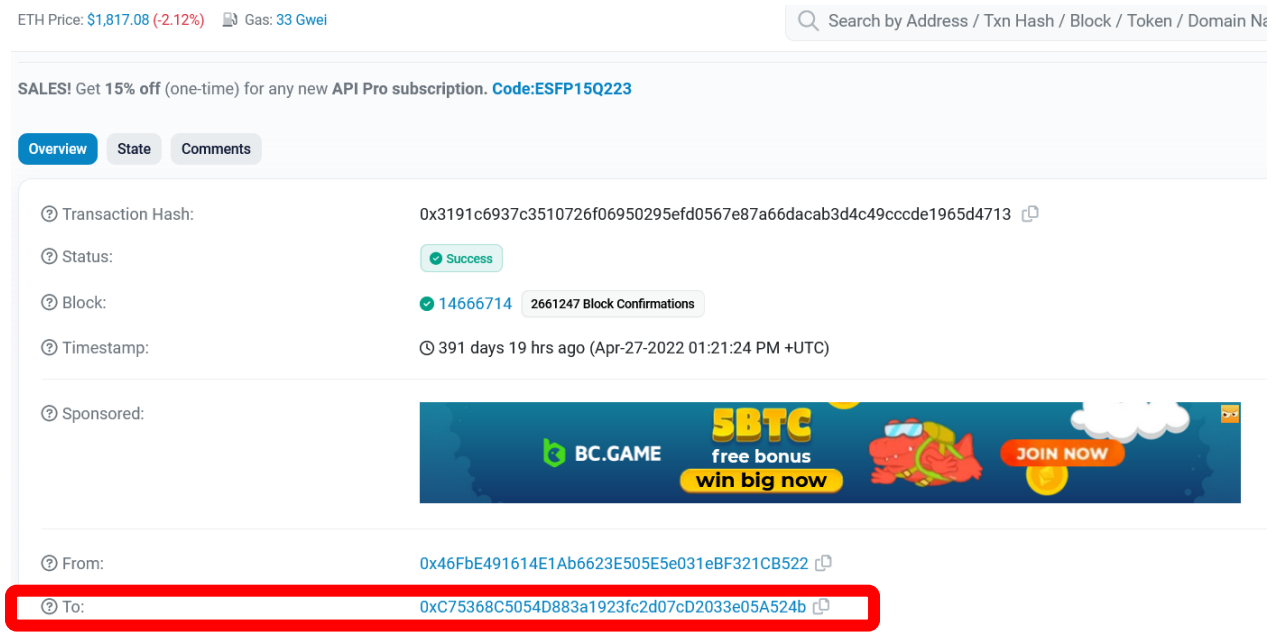


- 1 transaction entrante | pas de transactions sortantes

Penchons nous sur cette adresse

https://etherscan.io/txs?a=0xc40a8a6763969e88c8bf58a6e7a5adc61b8ebe11&f=2
https://etherscan.io/tx/0x3191c6937c3510726f06950295efd0567e87a66dacab3d4c49cccde1965d4713





- l'adresse de phishing 0xc40a…be11 est autorisée à approuver les adresses des victimes, elle transférera les fonds de la victime vers une autre adresse 0xc753…524b, pas elle-même.
- aucun transfert de jeton entrant ou sortant vers l'adresse de phishing.

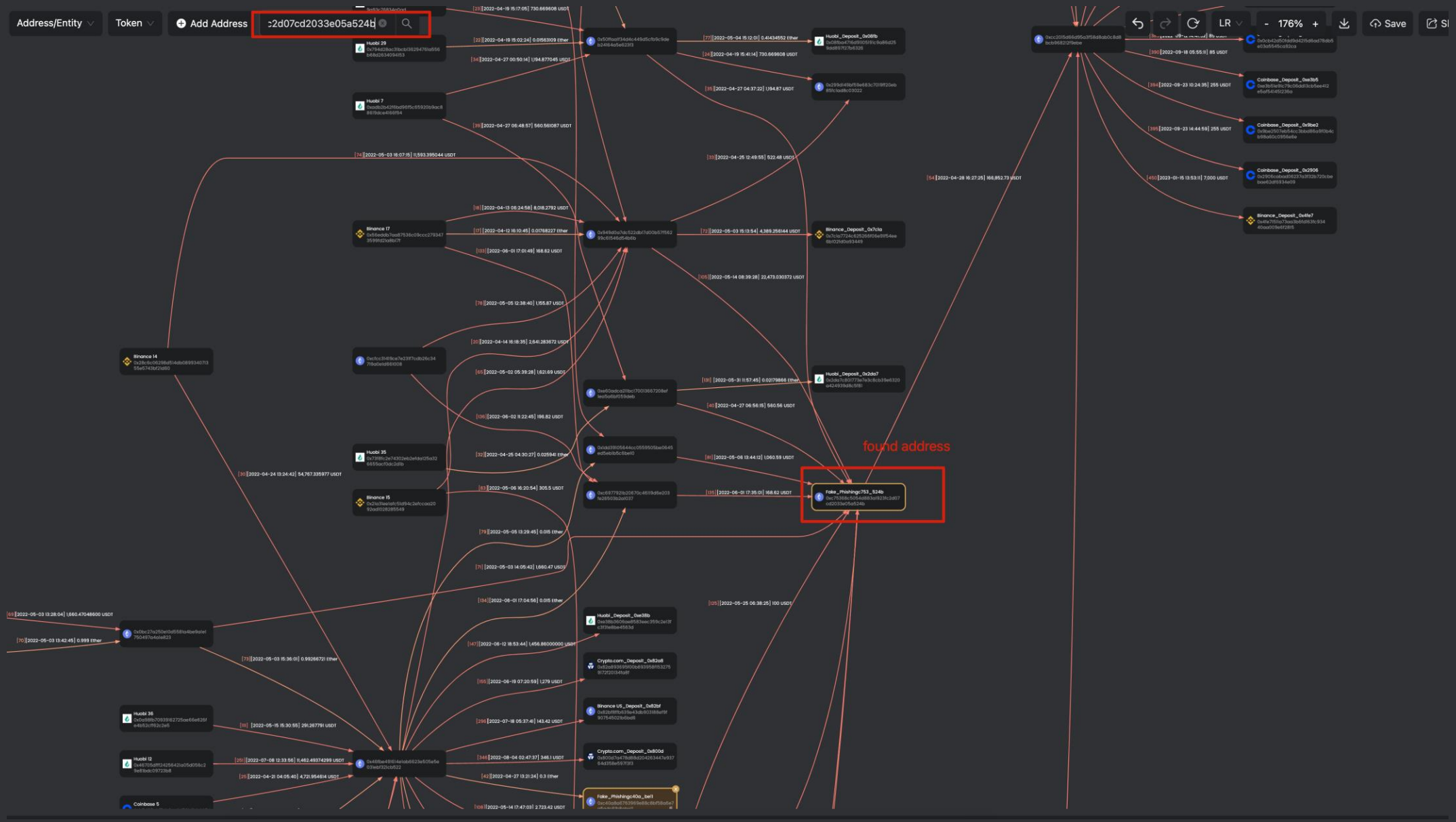
- l'Ether entrant de 0x46fb…b522 est pour les frais de gas pour transférer les fonds de la victime.

II. Atelier

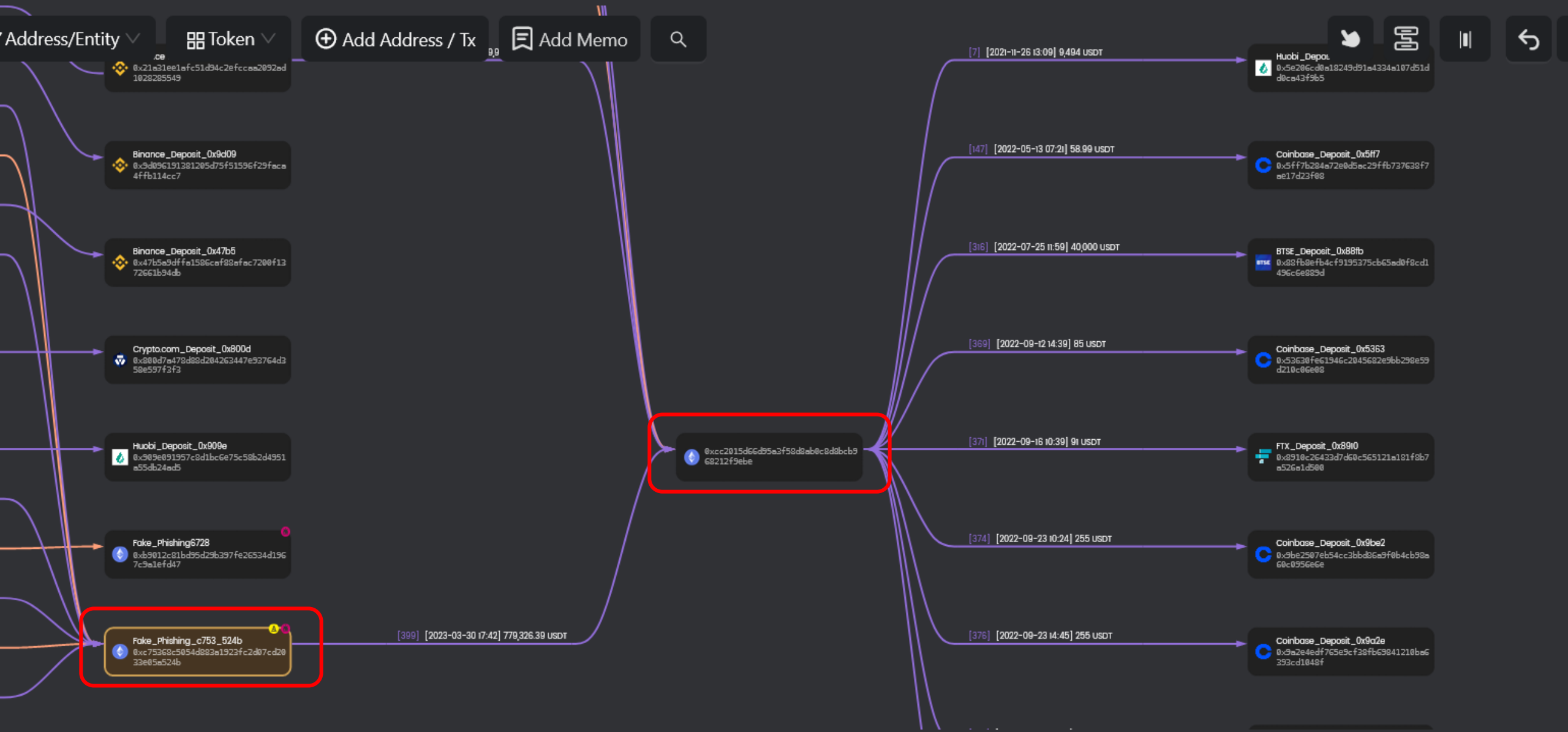
Notre carnet d'enquête :

- L'adresse où les fonds de Mathieu ont transité : 0xc40a...be11
  + C'est un leurre. Elle ne détient pas les fonds mais les transfert à une autre adresse : 0xc753...524b

https://metasleuth.io/result/eth/0xc75368c5054d883a1923fc2d07cd2033e05a524b



https://metasleuth.io/result/eth/0xc75368c5054d883a1923fc2d07cd2033e05a524b



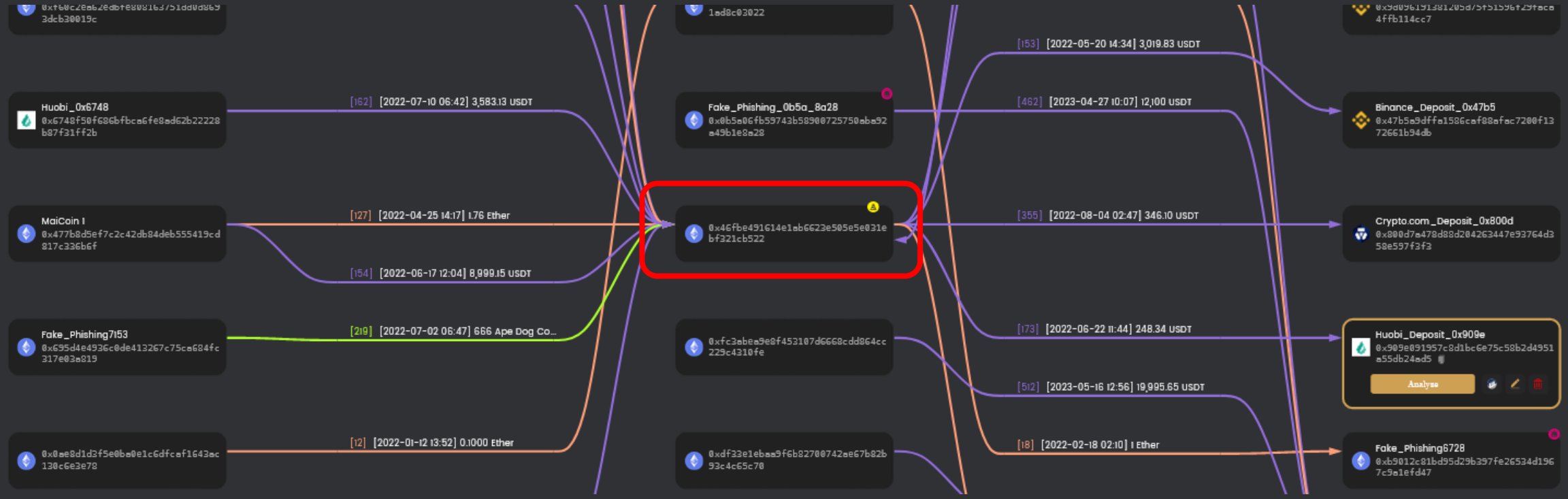
Notre carnet d'enquête :

- L'adresse où les fonds de Mathieu ont transité : 0xc40a...be11
  + C'est un leurre. Elle ne détient pas les fonds mais les transfert à une autre adresse : 0xc753...524b

- L'adresse 0x46fb...b522 est impliquée et sert à payer les frais pour transférer les fonds de 0xc40a...be11
  + Question : Est-ce que cette adresse appartient à l'attaquant ?

- Les fonds sont déposées sur l'adresse 0xcc20...9ebe.
  + Question : Est-ce que cette adresse appartient à l'attaquant ?

https://metasleuth.io/result/eth/0xc75368c5054d883a1923fc2d07cd2033e05a524b



- Flux : nombreuses transactions entrantes et sortantes
- Certaines proviennent de plateforme d’échange CEX (plateforme centralisée)
- Hypothèse : cette adresse serait rattachée à une plateforme d’échange « No-KYC ».

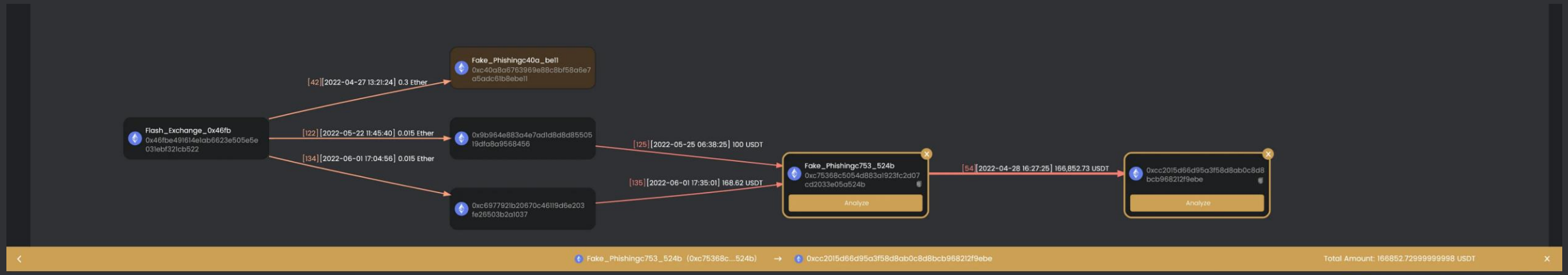
Notre carnet d'enquête :

- L'adresse où les fonds de Mathieu ont transité : 0xc40a…be11
    + C'est un leurre. Elle ne détient pas les fonds mais les transfert à une autre adresse : 0xc753…524b

- L'adresse 0x46fb…b522 est impliquée et sert à payer les frais pour transférer les fonds de 0xc40a…be11
    + Hypothèse : l'adresse serait rattachée à une plateforme d'échange « No-KYC »

- Les fonds sont déposées sur l'adresse 0xcc20…9ebe.
    + Question : L'adresse appartient à l'attaquant ?

https://metasleuth.io/result/eth/0xc75368c5054d883a1923fc2d07cd2033e05a524b



Date	Hash	From	To	Amount	Token	Note
2022-05-27 14:04:56	0x8a3a2bb....1c7a	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	9,900	USDT	
2022-06-25 04:46:32	0x80e1ea9....e87b	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	26,000	USDT	
2022-06-30 19:02:17	0x92f2632....4c34	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	2,043.8	USDT	
2022-07-31 16:04:44	0x61fe951....836f	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	2,021.71	USDT	
2022-10-31 18:46:11	0xb812fb4....53f9	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	3,737.46	USDT	
2022-12-01 00:06:47	0xe8ffd03....3fb7	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	164.88	USDT	
2023-01-12 18:00:47	0x293abda....88d6	0xc75368c5054d883a1923fc2d07cd2033e05a524b	0xcc2015d66d95a3f58d8ab0c8d8bcb968212f9ebe	13,000	USDT	

- Note sur l'affichage : les transfert de 0xc753…524b à **0xcc20…9ebe** sont fusionnés en une seule branche
- La dernière date de transfert correspond à une date proche de l'attaque avec des fonds similaires
- Le flux sortant est redirigé vers 83 adresses rattachées à des plateformes d'échange centralisées
- Hypothèse : cette adresse correspond à une plateforme d'échange « No-KYC »

II. Atelier

Notre carnet d'enquête :

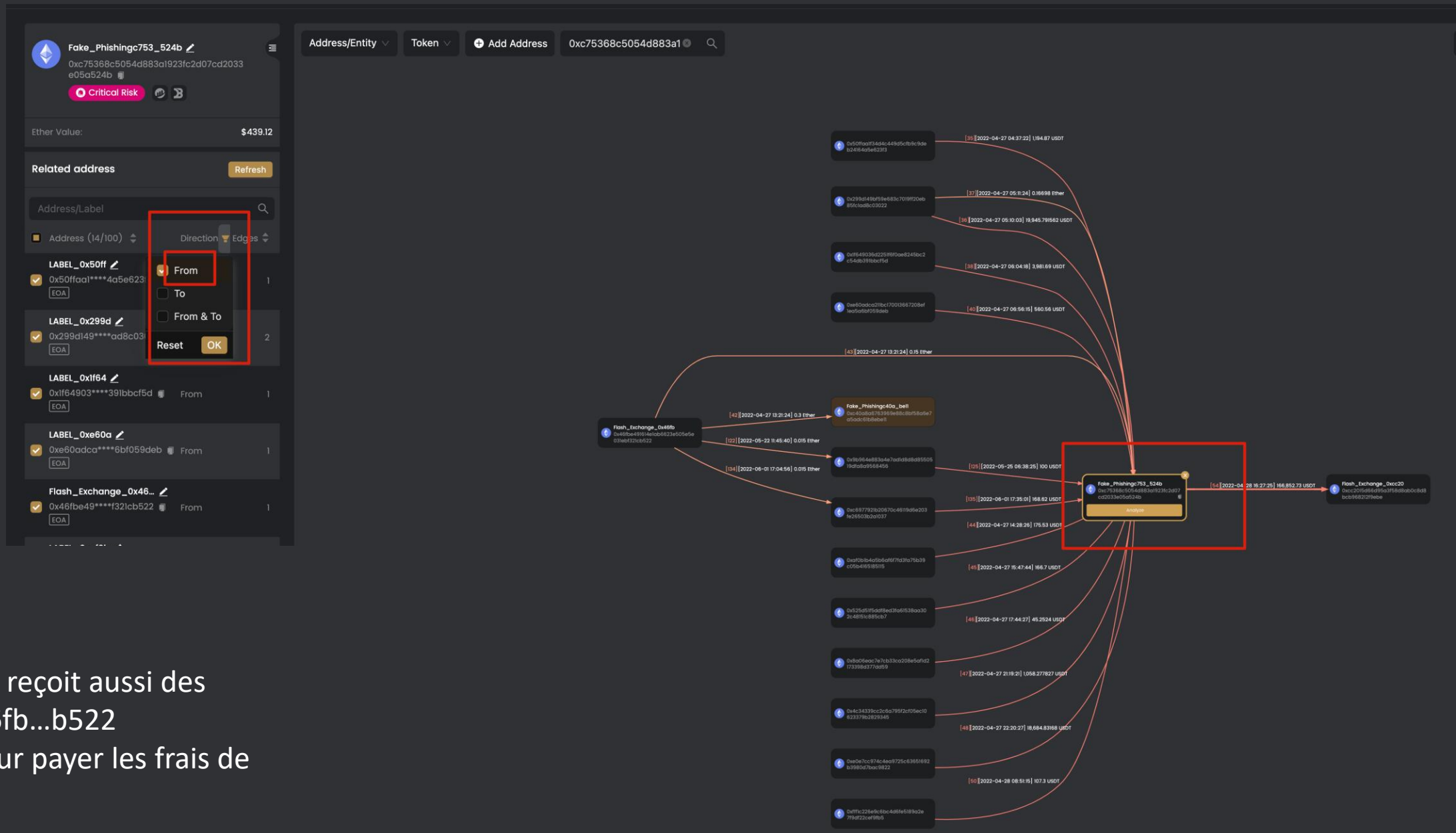
- L'adresse où les fonds de Mathieu ont transité : 0xc40a…be11
    + C'est un leurre. Elle ne détient pas les fonds mais les transfert à une autre adresse : 0xc753…524b

- L'adresse 0x46fb…b522 est impliquée et sert à payer les frais pour transférer les fonds de 0xc40a…be11
    + Hypothèse : l'adresse serait rattachée à une plateforme d'échange « No-KYC »

- Les fonds provenant de 0xc753…524b sont déposés sur l'adresse 0xcc20…9ebe.
    + Hypothèse : cette adresse correspond à une plateforme d'échange « No-KYC »

- Questions : En analysant d'autres victimes peut-on récupérer d'autres informations ?

https://metasleuth.io/result/eth/0xc75368c5054d883a1923fc2d07cd2033e05a524b



- 0xc753…524b reçoit aussi des fonds de 0x46fb…b522
- C’est aussi pour payer les frais de transactions

📖 Notre carnet d'enquête :

- L'adresse où les fonds de Mathieu ont transité : 0xc40a...be11
    + C'est un leurre. Elle ne détient pas les fonds mais les transfert à une autre adresse : 0xc753...524b

- L'adresse 0x46fb...b522 est impliquée et sert à payer les frais pour transférer les fonds de 0xc40a...be11
    + Hypothèse : l'adresse serait rattachée à une plateforme d'échange « No-KYC »

- Les fonds provenant de 0xc753...524b sont déposés sur l'adresse 0xcc20...9ebe.
    + Hypothèse : cette adresse correspond à une plateforme d'échange « No-KYC »

- L'adresse 0x46fb...b522 transfert aussi des fonds à 0xc753...524b pour payer ces frais de transactions : Nous avons mis en lumière le circuit utilisé par l'attaquant

Suite de l'enquête

Contexte : nous avons réussi à récolter un ensemble d'informations sur les méthodes de l'attaquant pour récupérer les fonds dérobés.

Objectif : Avec ces indices, nous cherchons d'autres informations.

Moyens :
- Se rapprocher des plateformes « No-KYC » que nous avons identifiés
- Consulter des bases de données pour identifier les propriétaires des wallets que nous aurons trouvés
- Employer d'autres sources d'informations et d'autres types d'outils d'investigation pour définir des adresses IPs , des adresses mails, des machines et autres

II. Atelier

M. X était à l'origine de cette campagne de phishing.

Est-ce que les utilisateurs malveillants peuvent complexifier les tâches des enquêteurs ?

III. Limites actuelles

Les utilisateurs malveillant peuvent faire de l'obfuscation d'information

Problématique : Les informations inscrites dans la blockchain sont immuables et persistantes dans le temps. Le contexte est favorable aux investigateurs.

Objectif : Pour se protéger, les utilisateurs malveillants vont tentés de rendre les informations de leurs passages plus difficiles à percevoir et à comprendre.

Exemples de moyens :

✂ **Peeling Chains :** Un portefeuille concentrant une grande quantité de crypto-actifs réalise une succession de transactions mineures pour transférer ses fonds sans alerter les services AMLs.

Chain Hopping : Convertir un crypto-actif avec un autre type de crypto-actif (par exemple du BTC contre de l'ETH).

⁉ **Anonymous Networks :** Réaliser des transaction à l'aide d'un réseau blockchain favorisant l'anonymat (ex: Monero).

Tumblers, Mixers and ConJoin: Le but de cette famille de méthodes est d'anonymiser des transactions. Les crypto-actifs sont mélangés avec d'autre crypto-actifs pour brouiller la lecture des transactions.

III. Limites actuelles

Notes sur les Mixers

Catégories	Types	Descriptions
Centralized custodial mixers	Centralisé, Custodian	Un des plus anciens (apparition vers 2011). Ils sont gérés par un nombre restreint d'opérateurs. Ces mixers sont centralisés et "custodians".
CoinJoins Mixer	Décentralisé, No Custodian	Les utilisateurs disposent de wallets avec une forte anonymisation. Pour réaliser ces transactions, ces mixers combinent plusieurs fonds de plusieurs utilisateurs dans une seule et même transaction.
Smart contract mixers	Décentralisé, No Custodian	L'utilisateur confie ses fonds au mixer et reçoit une preuve cryptographique pour montrer qu'il est propriétaire de ses fonds. L'utilisateur peut envoyer ou retirer ses fonds quand il le souhaite. Tant que les fonds sont stockés sur le mixer, ils sont « brassés » plusieurs fois.

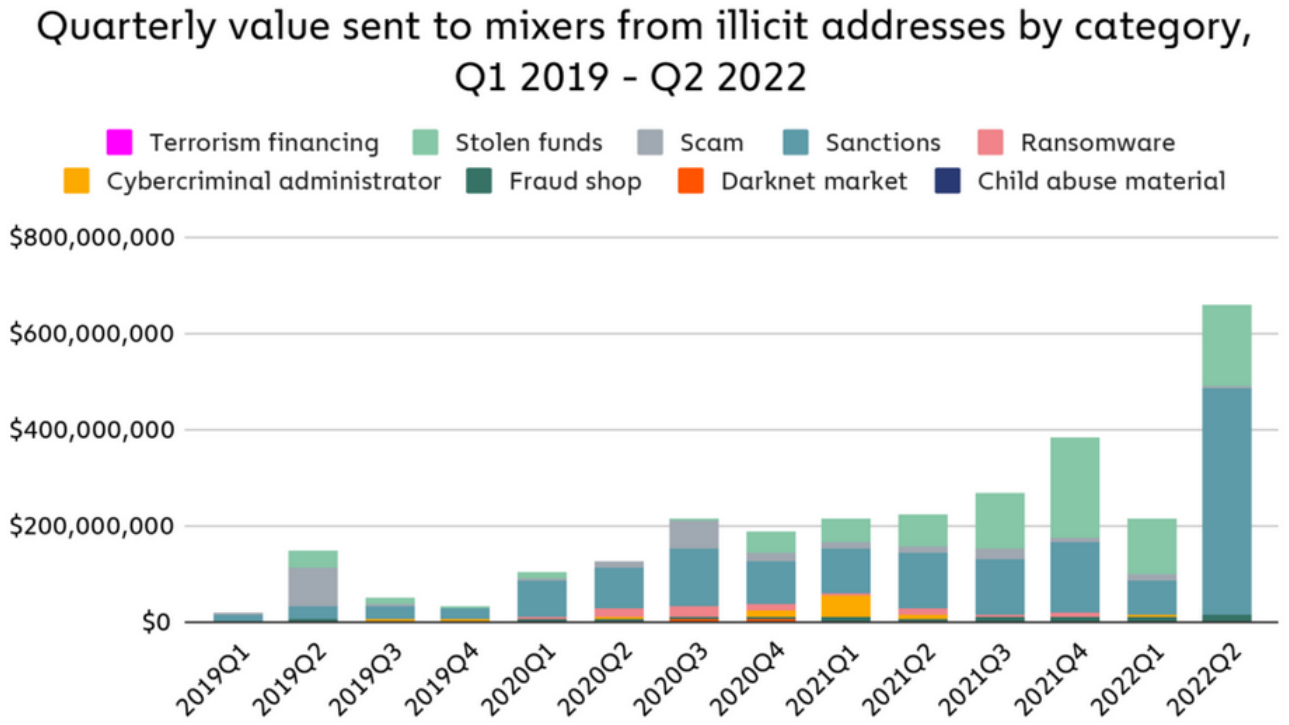
III. Limites actuelles

Notes sur les Mixers

Usage :

- D'après un article de ChainAnalysis paru le 14 juillet 2022, les adresses identifiées comme illicites ont transféré près de 10% de leurs fonds vers des Mixers.

- D'après la même étude, 23 % des fonds envoyés aux mixers sont des fonds illicites (composition des fonds d'origine illicite >>>).



Source : https://blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/

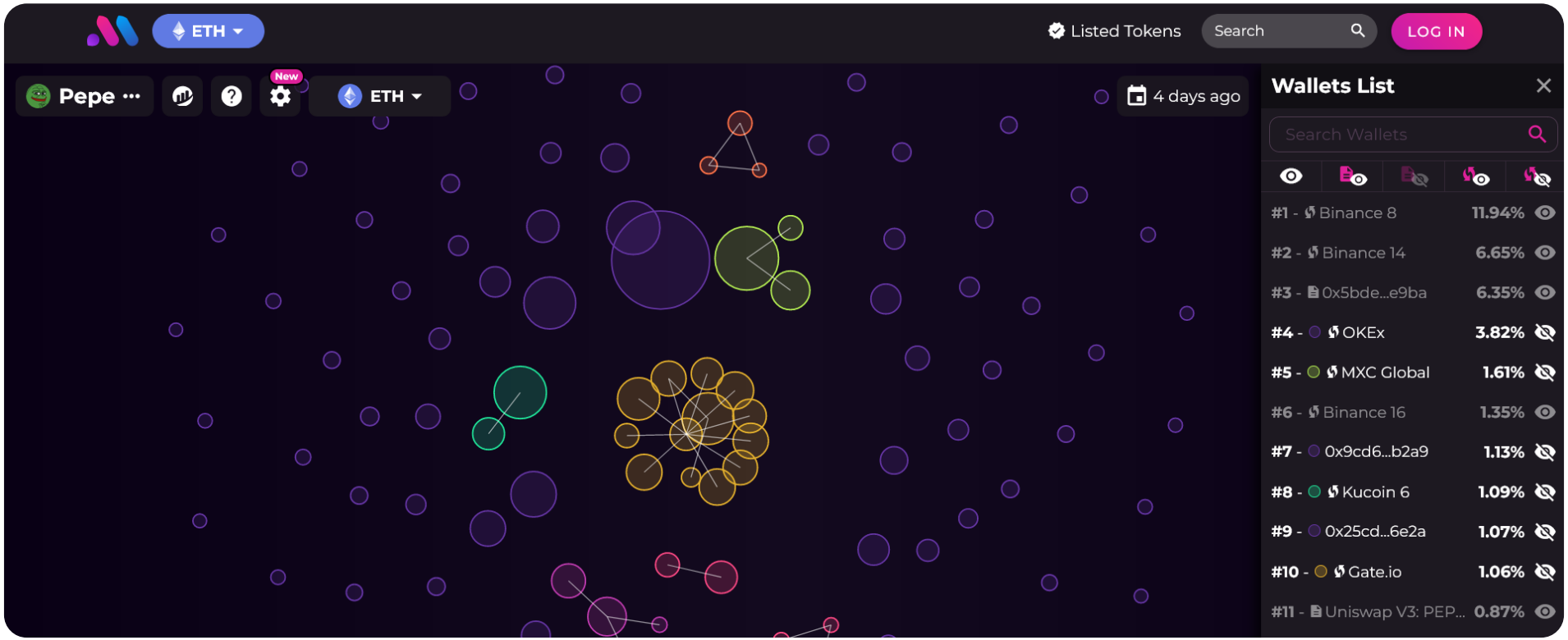
Merci de votre attention

https://lab.setinstone.io

Thomas BENOIT / CEO SET IN STONE
thomas.benoit@setinstone.io

ANNEXE

IV. Analyse des relations entre portefeuilles



https://app.bubblemaps.io/eth/token/0x6982508145454ce325ddbe47a25d4ec3d2311933